## REMARKS

I. STATUS OF CLAIMS

Claims 1-2, 5-14, 17-26, and 29-36 are pending in the Application. Claims 3, 4, 15, 16, 27, and 28 have been canceled. It should be noted that Applicant has elected to amend said Claims solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making this amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled and does not concede, in any way, that the subject matter of such Claims was in fact taught or disclosed by the cited prior art. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

II. REJECTION BASED ON 35 U.S.C. §102(e)

The Office Action has rejected Claims 1-36 under 35 U.S.C. 102(e) as being anticipated by McManis (U.S. Pat. No. 5,757,914). The rejection is respectfully traversed.

Claims 1, 13, and 25 have been amended to clarify the invention. Claims 1, 13, and 25 now incorporate the elements of Claims 3, 4, and 15, 16, and 27, 28, respectively. No new matter has been added. Claims 1, 13, and 25 appear as follows:

1. A method of securely invoking an access control function, the method comprising the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

generating a mapping between access control events and access control functions;

detecting that an access control event has occurred;

determining that the access control event is mapped to the access control function;

retrieving an executable element if the access control event is mapped to the access control function;

generating a digital signature for the retrieved executable element;

determining whether the retrieved executable element matches the access control function by comparing the digital signature of the retrieved executable element and the digital signature for the access control function; and

executing the retrieved executable element only when the retrieved executable element matches the access control function.

13. A computer-readable medium carrying one or more sequences of one or more instructions for securely invoking an access control function, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

generating a mapping between access control events and access control functions;

detecting that an access control event has occurred;

determining that the access control event is mapped to the access control function;

retrieving an executable element if the access control event is mapped to the access control function;

generating a digital signature for the retrieved executable element;

determining whether the retrieved executable element matches the access control function by comparing the digital signature of the retrieved executable element and the digital signature for the access control function; and

executing the retrieved executable element only when the retrieved executable element matches the access control function.

25. An access control system, comprising:

a processor;

a memory coupled to the processor;

a first mapping that maps each of a set of access control functions to a digital signature of that access control function;

the processor configured to retrieve an executable element in response to a request to execute a first access control function;

the processor configured to generate a mapping between access control events and access control functions;

the processor configured to detect that an access control event has occurred;

the processor configured to determine that the access control event is mapped to the access control function;

the processor configured to retrieve an executable element if the access control event is mapped to the access control function;

the processor configured to generate a digital signature for the retrieved executable element;

the processor configured to determine whether the retrieved executable element matches the first access control function by comparing the digital signature of the retrieved executable element and the digital signature for the first access control function; and

the processor configured to execute the retrieved executable element when the retrieved executable element matches the first access control function.

Since Claim 1 has incorporated the elements of Claims 3 and 4, the Office Action rejections of those claim elements will be addressed. In particular, McManis does not teach or disclose a system that generates a mapping between access control events and access control functions as claimed in Claims 1, 13, and 25. There is no disclosure of access control events in McManis, nor does McManis disclose generating a mapping between access control events and access control functions. McManis teaches a program module verifier. Therefore McManis does not contemplate such a system. The Office Action generally refers to McManis with respect to Claim 4, but does not detail the rejection with particularity.

The Office Action does not address the element of Claim 4 that determines that the access control event is mapped to the access control function. McManis does not disclose generating a mapping between access control events and access control functions. Therefore, McManis does not disclose or contemplate determining that the access control event is mapped to the access control function because no such mechanism could be taught by McManis when the generation of a mapping is not contemplated in McManis.

Additionally, with respect to Claim 3, the Office Action states that "McManis discloses wherein the method further includes the step of detecting that an access control event has occurred ... (see col. 3, lines 59-67, col. 4, lines 1-15)". However there is no mention of such a detection in McManis. McManis teaches that a procedure can executed. This has no relationship to detecting that an access control event has occurred. Col. 3, line 59-col. 4, line 15 states:

> "Referring to FIGS. 2 and 3, an executable procedure (e.g., the "main application A procedure" 128-A in FIG. 1) in program module A begins execution (step 200). For the purposes of this discussion, the procedure in program module A that is being executed will be called "procedure A" and the procedure that it is attempting to call in program module B will be called "procedure B".
>
> Prior to making a procedure call to an executable procedure in program module B (step 220), procedure A makes a procedure call to the verifier to request verification of the authenticity of program module B (step 202). The verifier then attempts to verify the authenticity of program module B and sends a return value to procedure A to indicate whether or not the verification of program module B was successful (step 204).
>
> More specifically, the verifier, which is preferably a distinct trusted object (or alternately a trusted system service procedure) receives the request message from

procedure A (step 206), and decodes (step 208) a digital signature embedded in program module B using a public key provided by the calling procedure (i.e., procedure A). The public key provided by calling procedure A to the verifier is the "group" public key 126-A embedded in program module A."

McManis clearly does not teach or disclose detecting that an access control event has occurred. McManis does not address access control events, nor does he disclose the detection of such events. Therefore, McManis does not contemplate such a feature.

The Office Action further states that "McManis discloses ... and wherein the step of retrieving the executable element is performed in response to detecting that the event has occurred (see col. 3, lines 59-67, col. 4, lines 1-15)". However, as noted above, McManis does not contemplate detecting that an access control event has occurred. Without such detection, McManis could not teach or disclose what the Office Action states. There is no relationship between McManis' teaching that a procedure can be executed and Claim 1's element of retrieving an executable element if the access control event is mapped to the access control function.

McManis therefore does not teach every aspect of the claimed invention.

In a proper rejection under § 102(e) the cited reference must show each and every claimed feature in the same combination as arranged in the claim. See Lewmar Marine, Inc. v. Barient, Inc., 827 F.2d 744, 747-48, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987). If even a single element or limitation is missing from the reference, anticipation is not found. Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Claims 1, 13, and 25 are therefore allowable. Claims 2, 5-12 and 14, 17-24 and 26, 29-36 are dependent upon Claims 1, 13, and 25, respectively, and are allowable. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. 102(e).

III. CONCLUSIONS & MISCELLANEOUS

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

The Applicants believe that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments herein and further examination on the merits are respectfully requested.

The Examiner is invited to telephone the undersigned at (408) 414-1214 to discuss any issue that may advance prosecution.

No fee is believed to be due specifically in connection with this Reply. To the extent necessary, Applicants petition for an extension of time under 37 C.F.R. § 1.136. The Commissioner is authorized to charge any fee that may be due in connection with this Reply to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: July 5, 2005

Kirk D. Wong
Reg. No. 43,284

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 214
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on July 5, 2005 by Trudy Braglon